Bittium Tough Mobile™ 2
Multicontainer

Multicontainer feature brings added versatility and ease of use to the secure Bittium Tough Mobile 2 smartphone. The containers are run on a secure platform making it different from the typical smartphones where a container is used to protect the data on an inherently insecure platform.

Multicontainer enables use of up to four container workspaces with the Tough Mobile 2 smartphone, which means that the user can access the data of e.g. four different organizations. The workspaces are securely isolated from each other, and all the connections, services and applications from the workspaces are running and online simultaneously.

Each workspace has a unique appearance, which makes it easy to identify which container is being used. Switching from workspace to another is done by swiping from the home screen.

FOR MORE INFORMATION, PLEASE CONTACT:
sales1global@bittium.com

Benefits

Sensitive Data Secured

The most secure mobile platform for keeping sensitive data safe.

Use Trusted and Public Services with Same Device

Each container has own security policy for data isolation.

Versatility

A Multicontainer solution for professional and personal use with up to four parallel workspaces within one device.

Secure Connectivity and Trusted Device Management

With Bittium Secure Suite services.

Easy to Use

Easily access workspaces and switch between them by swiping from the home screen without the need for additional passwords or PIN codes.

Bittium Tough Mobile™ 2
Multicontainer

Secure Connectivity to Background Services

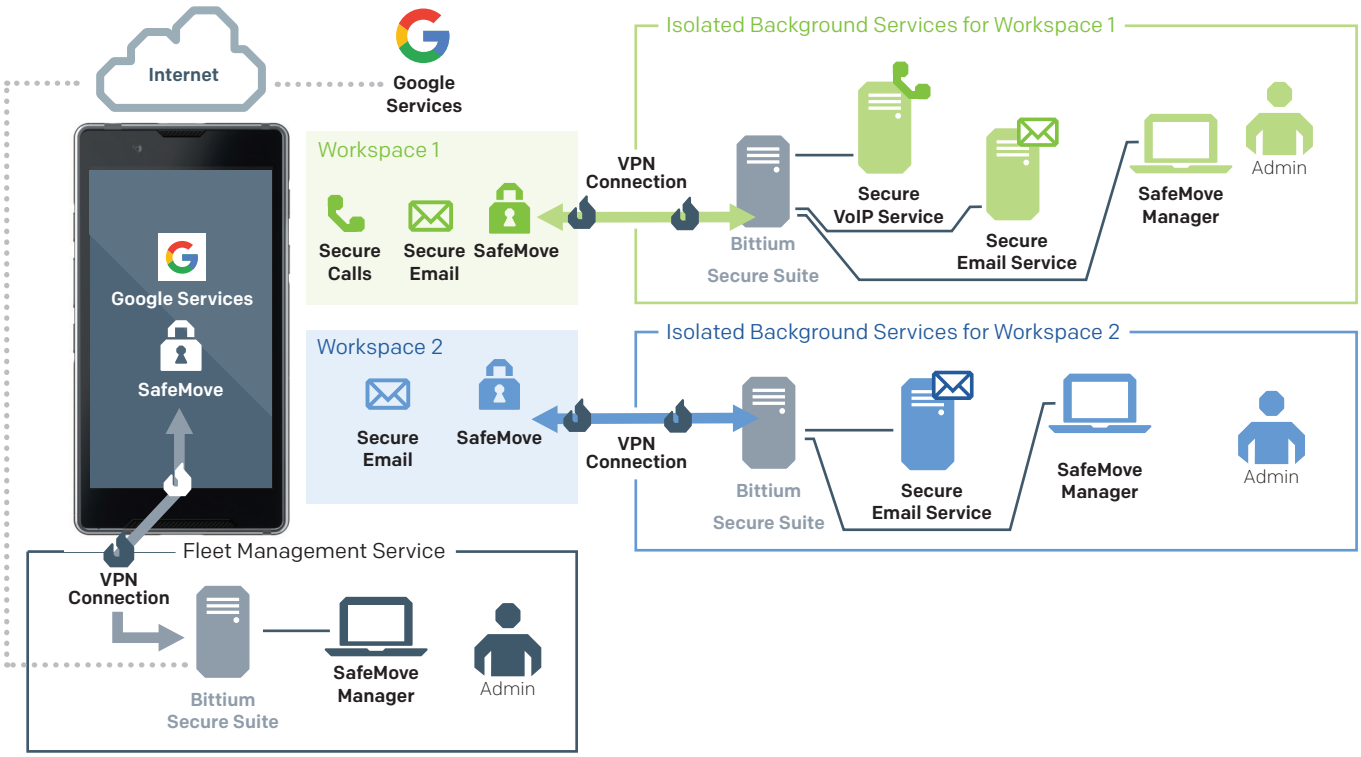
- Up to four isolated and simultaneous containers and home screen
- The workspaces are running on secure platform and are securely isolated from each other
- Each container has a dedicated, secure VPN connection, and all applications in the container use the VPN connection
- The network behind the VPN connection can be a closed/private network, or an open network to the public internet, depending on the network configuration
- Applications can access any data and services available through the network behind the VPN connection
- No need for additional authentication when switching between the workspaces

Trusted Device Management

- All device and container configurations can be done online by an administrator
- Each organization can provide their vetted applications for the organization specific container
- Protection of classified data and services from malicious apps

Use Cases

- **Use case 1: Business and personal phone in the same**
  - Home screen for personal use and applications
  - Container for business data
  - Business data, personal data and network traffic for both are isolated from each other
- **Use case 2: Access to sensitive data of different organizations from the same device**
  - When user's work requires accessing data of different organizations
  - Each container has a dedicated VPN connection to each organization's network



Bittium • Ritaharjuntie 1, FI-90590 Oulu, Finland • Tel. +358 40 344 2000 • **www.bittium.com**